SHEET 1 OF 5

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

Ral

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

ATTY.	DOCKET	NO.

500.41092X00

SERIAL NO.

APPLICANT

M. NISHIOKA, et al

FILING DATE January 16, 2002 GROUP 2136

U.S. PATENT DOCUMENTS FILING DATE IF APPROPRIATE SUBCLASS CLASS NAME DATE EXAMINER DOCUMENT NUMBER INITIAL FOREIGN PATENT DOCUMENTS ABSTRACT SUBCLASS CLASS COUNTRY DOCUMENT NUMBER NO YES OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.) R. L. Rivest, et al "A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, vol. 21, No. 2. pp. 120-125, 1978. Rese V. S. Miller, Use of elliptic curves in Cryptography, Proc. of Crypto '85, LNCS218, Springer-262 Verlag, pp. 417-426, 1985. N. Koblitz, Elliptic Curve Crytosystems, Math. Comp. 48, 177, pp. 203-209, 1987.

EXAMINER EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

DATE CONSIDERED

1/31/2006

FORM F	TO-	1449	U.S.	. Dep	artme	ent of			ATTY.	DOCKET NO.		SE	RIAL NO.	BADEMAN	SE S	
Commerc	e Pa	tent a	nd Tr	adem	ark C	Office)		500.4	500.41092X00 10/046,224						
٠	INF ST	ORMA	ATION ENT I	I DISC BY AF	PLIC	URE ANT			APPLIC M. NI	CANT SHIOKA, et al		ı				
	(Use sev	eral sh	eets if (necessa	ıry)	_		FILING Janua	DATE ary 16, 2002		1	36			
						U.S	. PA	TENT	DOCL	JMENTS						
EXAMINER INITIAL		DOCUME	NT NUM	BER					DATE	NAME	CLASS		SUBCLASS	FILING DATE IF APPROPRIATE		
NI IAC											┼					
						_		}				-				
											+-	-				
								+								
				}						201	か ^で	V	7			
	╁—										1	-4	3			
	╁				-					100 C						
	┼-	-									_					
	-															
	┼	-														
			NT F		IME	NTS	L									
FORE	GNI	1	MENT N		JIVIL	110			DATE	COUNTRY	c	LASS	SUBCLASS	ABSTRACT		
					,		τ			 				YES	NO	
			ļ			 -	 				\dashv		 	 		
	_		ļ	<u> </u>	<u> </u>	-	┼						 	 		
		-	<u> </u>	 	 		┼				_					
				-	-		+-	 			_		1			
		+-	┼	-	┼	+-	 	+-	 	+						
						1		hor ¹	Citle D	ate. Pertinent	Page	s, E	tc.)			
OTHE	R D	<u>ocul</u>	MEN.	<u>15 (l</u>	nclu	uing	Auti	ne and	Public-	ate, Pertinent key Encryptions	as Int	racti	able as Fac	torization	, MIT	
Lac		ΙTΑ	chnic	al Re	port.	MI 1/L	.C3 [r	KWMOI	11133101							
Rec	7							4		nd a Signature So heory, IT-31, 4, p	heme p. 469	Bas -472	sed on Disc , 1985.			
1060		S.	Gold	wass	er, et	al Pr	obabi	listic E	Encrypti	on, JCSS, 28, 2, j	op. 270	0-29	9, 1984.			
EXAM	INER	$\overline{}$		1	7	>			ONSIDE	RED 1/3	120	00	<u> </u>			
EXAM	INER			itatio	n is co	onsid	lered,	draw	line thre	ough citation if no	ot in c ant.	onfo	rmance ar	nd not		
consi	derec	i. Incl	uae c	ору с		10111	. 4101	,,,,,,,		(Form PTO-14						

SHEET 3 OF 5 SERIAL NO. ATTY. DOCKET NO. FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office 10/046,224 500.41092X00 INFORMATION DISCLOSURE APPLICANT STATEMENT BY APPLICANT M. NISHIOKA, et al GROUP FILING DATE January 16, 2002 (Use several sheets if necessary) 2136

	(U	se sev	GISI 21	ieem ii	1100000	,,			Janua	ry 16, 2	002		36		
						U.S	. PA	ENT	DOCU	MENT	s				
EXAMINER			ENT NUI	MER					DATE		AME	CLASS	SUBCLASS	FILING DAT	E ATE
INITIAL		DOCUM	ENT NO	WDEN.								 			
	+-+	十										1			
	++							\top				1			
	╁╾┼	+											\sqrt{I}		
	╂╾╅						$\neg \uparrow$				26	110	71—		
	+ 1											111			
	+													 	
	╅╾┪			-								_		 	
	+														
			-	┢	 									 	
			\vdash	1	†								<u> </u>	1	
				DOC	IIME	NTS	<u> </u>								
FORE	IGN F	l l		NUMBER					DATE		COUNTRY	CLASS	SUBCLASS	ABSTRACT	l
		BOC	DWENT							 			 	YES	NO
			T						ļ	 			 	-	
]					 					
							<u> </u>		<u> </u>	<u> </u>					<u> </u>
OTH	R DO	CU	MEN	ITS (Inclu	ding	Auth	or,	Title, Da	te, Pe	rtinent P	ages, E	tc.)		
266	- 1										Encryptio er-Verlag,			des all Par	тіаі ———
100	2	s.	Gold	iwass	er, et	al, Le	cture	Note	s on Cry	tograp	hy, http://	vww-cse, 			
26	2				-4-1	A =0	Dub	lic-ke lag, p	y Crypto p. 308-31	system 8, 1998			oring, Proc	of Euroc	rypt
EXAM	AINER			A	1		D	ATE C	ONSIDE	RED	1/31/	2 00	<u> </u>		

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. (Form PTO-1449 [6-4])

EXAMINER

NOV 1 7 2005 SHEET 4 OF 5 SERIAL ATTY. DOCKET NO. 10/046,224 500.41092X00 APPLICANT
M. NISHIOKA, et al

FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)									FILING DATE January 16, 2002 GROUP 2136						
						υ.s.	PA	TENT	DOC	JMENT	<u> </u>	T	T -		
XAMINER	Τ.	OCUMEN	T NUMB	ER					DATE	N/	NAME	CLASS	SUBCLASS	FILING DAT	ATE
NITIAL	-13	OCOMILIA I										-	 		
	十	_											 	 	
	-+-	\dashv	_	_	\top							 		 	
	+	十	-	+	十								D) //	 	
			-		_	-+							7	 	
	-+	-+	\dashv	\dashv	\dashv	\dashv									
	-+		\dashv	\dashv	-+	十	\neg								
	_			}	-+									<u> </u>	
					L			1		_1			_		
FOREIG	N P	ATEN	IT D	<u>ocu</u>	MEN	ITS_			DATE	1 6	OUNTRY	CLAS	S SUBCLASS	ABSTRACT	
	.	DOCUM	ENT NU	MBER					DATE					YES	NO
															├-
	\vdash														-
							_	1							┼-
							-	1							╁-
							├─	+	1	_					1_
					-	├	+-	+	+						丄
				L		<u> </u>	<u> </u>				tinont l		Etc.)		
OTHER	DO	CUN	IENT	rs (Ir	nclud	ling	Aut	hor,	Title, D	ate, Pe	America d	CM S.	mnosium on	Theory of	F
JCQ		D. I	olve	, et al	Non-	-Malle	eable	Cryp	tograph	y, in 23	Annual /			ertext Atta	
DOOR		M. Pro	Naor, oc. of	et al	Publi C, AC	ic-key M Pro	y Cry ess,	ptosy pp. 42	stems F 7-437, 1	Provably 990.	Secure A	gainst	Chosen Ciph	oc. of Euro	
DOL		7			-1.00	-4i	al Ae	vmm	etric End 5. 92-111	cryption I		ncrypt V	vith RSA, Pr		

EXAMINER EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

DATE CONSIDERED

(Form PTO-1449 [6-4])

1/31/2006

NOV J 7 2005 SHEET 5 OF 5 SERIAL NO. ATTY, DOCKET NO. FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office 10/046,224 500.41092X00 INFORMATION DISCLOSURE APPLICANT STATEMENT BY APPLICANT M. NISHIOKA, et al GROUP FILING DATE (Use several sheets if necessary) 2136 January 16, 2002 U.S. PATENT DOCUMENTS FILING DATE SUBCLASS EXAMINER DATE DOCUMENT NUMBER INITIAL FOREIGN PATENT DOCUMENTS SUBCLASS ABSTRACT CLASS COUNTRY DATE DOCUMENT NUMBER NO OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.) R. Cramer et al, A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack, Proc. of Crypto '98, LNCS1462, Springer-Verlag, pp. 13-25, 1998. El

M. Bellare, et al Relations Among Notions of Security for Public-key Encryption Schemes, Proc. 00 of Crypto '98, LNCS1462, Springer Verlag, pp. 26-45, 1998. 1/31/2006 DATE CONSIDERED EXAMINER ;

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Form PTO-1449 [6-4])